

# Separability, entanglement and full families of commuting normal matrices

Jan Samsonowicz<sup>1</sup>, Marek Kuś<sup>2</sup>, and Maciej Lewenstein<sup>3</sup>

<sup>1</sup>*Warsaw University of Technology, Faculty of Mathematics and Information Science, Pl. Politechniki 1, 00-61 Warszawa, Poland*

<sup>2</sup>*Center for Theoretical Physics PAS, Al. Lotników 32/46, 02-668 Warszawa, Poland*

<sup>3</sup>*ICREA and ICFO - Institut de Ciències Fotòniques, Parc Mediterrani de la Tecnologia, Castelldefels, 08860 Spain\**

(Dated: February 1, 2008)

We reduce the question whether a given quantum mixed state is separable or entangled to the problem of existence of a certain *full family of commuting normal matrices* whose matrix elements are partially determined by components of the pure states constituting a decomposition of the considered mixture. The method reproduces many known entanglement and/or separability criteria, and provides yet another geometrical characterization of mixed separable states.

PACS numbers: 03.67.Mn, 03.65.Ud

## I. INTRODUCTION

**Entanglement and separability problem.** Entanglement is the most important quantum phenomenon, responsible for genuine, distinct and unique properties of the quantum world, and possibilities this world offers for future technological applications, such as quantum engineering, and quantum information [1]. Despite enormous efforts, many fundamental questions concerning entanglement remain open (for an excellent recent review see [2], and [3] for some general geometric settings of the problem). In the seminal paper in 1989 Werner [4] gave the definition of separable (i.e. non-entangled) states: a state of a bi-partite system is separable iff it is a mixture of pure product states. A simple question: given a state, is it separable or not, is known as the *separability problem*. Only in very rare instances we know operational sufficient and necessary criteria (SNC) that allow to solve this problem:

- for  $2 \times 2$  (two qubit) and  $2 \times 3$  (qubit-qutrit) systems the SNC are given by the positive definiteness of the partial transform [5]; this is the famous PPT criterion, introduced by Peres as necessary for separability in Ref. [6].
- for 3 qubit symmetric ("bosonic") states PPT criterion is also SNC [7].
- for continuous variables  $1 \times 1$  (one mode per party) Gaussian states, PPT criterion (formulated at the level of correlation matrices) is a SNC [8, 9].
- for continuous variables  $m \times n$  (all bipartite) Gaussian states there exist an operational SNC based on recursion for correlations matrices [10].
- for continuous variables tripartite  $1 \times 1 \times 1$  Gaussian states there exist an operational SNC based on "iteration" of PPT condition for correlations matrices [11].

In general we have to rely either on only necessary criteria, or only sufficient ones, or on numerical approaches. Although there exist very efficient numerical procedures that employ optimization methods of semi-definite programming [12], the complexity of the problem grows with the dimensionality of the underlying Hilbert spaces: in fact it has been proven that the problem belongs to the complexity NP-class [13].

**Reformulations of the separability problem.** The market for only necessary, or only sufficient criteria is growing constantly, and it is impossible to review it in a non-review style article (for this reason we recommend the readers the review [2]). There are also many attempts to reformulate the problem of separability in different mathematical terms. A paradigm example for such an approach is the formulation of the separability problem in terms of positive maps due to Horodeccy [5]. A state is entangled iff there exist a positive map acting on, say, Alice, such that when applied to the state in question, it produces a non-positive definite operator. Similar approach deals with entanglement witnesses, i.e. observables that have positive averages on all separable states, but a negative average on some entangled state: A state is entangled iff there exist a witness operator that detects it, i.e. has a

---

\*Electronic address: J.Samsonowicz@alpha.mini.pw.edu.pl; Marek.Kus@cft.edu.pl; Maciej.Lewenstein@icfo.es

negative average. Obviously both these approaches are not operational, but nevertheless they are extremely useful, since they allow to generate many necessary separability (sufficient entanglement) criteria via explicit construction of positive maps [14], witnesses [15], and methods of their (local) measurements (cf. [16], respectively).

We have recently presented another example of the reformulation of the separability problem employing harmonic analysis on compact groups [17]. In this approach quantum mechanical states are replaced by non-commutative characteristic functions defined on the considered group, and separability problem reduces to the question whether a characteristic function defined on a product group of two groups can be represented as a mixture of products of characteristic functions on each of the individual groups. The present paper is in a sense similar to the Ref. [17]: we present yet another reformulation of the separability problem and reduce it to an apparently unrelated question of existence of a *full* (in a sense specified below) *family of commuting normal matrices*, whose matrix elements are partially determined by components of the pure states that constitute a decomposition of the considered mixed state.

**Decompositions of mixed states.** A given genuine (not pure) mixed state  $\rho$  has infinite number of decompositions in terms of projectors onto pure states. This fact has been already recognized by Schrödinger in 1935 [18], and elaborated thoroughly from the more modern view by Hughston *et al.* [19]. Any decomposition of a density matrix of rank  $r$  into  $K$  projectors can be described in terms of a rectangular  $K \times r$  matrix, whose  $r$  columns are orthonormal. Such objects are known in geometry to form a so called  $V_{K,r} = U(K)/U(K-r)$  Stiefel manifold [20]. Separability problem might be also formulated as a problem of statistical mechanics of a fictitious systems on the Stiefel manifold, characterized by a positive definite Hamiltonian (cost-function) that vanishes for separable states [21]. Here, we follow another avenue: we consider all decomposition of  $\rho$  into  $K$  terms for sufficiently large  $K$ : such decompositions are related via unitary transformations  $U(K)$ . The matrix elements of the density matrix, on the other hand, form a Gram matrix of scalar products of certain vectors from this  $K$  dimensional space. The first chapter of the paper is thus devoted to the study of such Gram decompositions. It provides complementary results to the Ref. [19].

**Plan of the paper.** As stated above, Section II is devoted to the Gram decompositions, and its main result is the Theorem 1, that describes how the two different Gram decomposition are connected. We present a reformulation of the separability problem in Section III, in the Theorem 2. Here, an example of so called Werner matrices [4] is elaborated in detail. The section IV contains the main result of this paper: a novel (but unfortunately not immediately operational) SNC for separability in terms of existence of what we call a *full family of commuting normal matrices (FFCNM)* (Theorem 3). We specify this result to the particularly simple case of  $2 \times N$  systems, where the separability SNC requires existence of a single normal matrix, whose matrix elements are partially known. Here we use the general properties of the density matrices in  $2 \times N$  systems (as presented in Appendix) and formulate elegant theorems on the existence of normal extensions of partially known matrices based on earlier and some new results for  $2 \times 2$ , and  $2 \times 3$ . We discuss also application of our criterion to PPT entangled states of rank 5 in  $2 \times 4$  systems. We relate these results to the theory of generalized concurrence [22].

## II. GRAM DECOMPOSITIONS OF DENSITY MATRICES

**Decompositions of density matrices.** Physical states of composite quantum systems are represented by density matrices, i.e. Hermitian, positive definite linear operators of trace one, acting in the Hilbert space  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \dots$ , which is a tensor product of Hilbert spaces corresponding to subsystems  $A, B, \dots$  of the considered system. In the following we shall be concerned with states of bipartite systems in a finite-dimensional Hilbert space i.e. described by positive definite Hermitian density matrices  $\rho = \rho^\dagger \geq 0$  with  $\text{Tr} \rho = 1$ , acting on the Hilbert space of the composite system  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ . Without loosing generality we will assume that  $\dim \mathcal{H}_A = M \geq 2$  and  $\dim \mathcal{H}_B = N \geq M$ , i.e.  $\mathcal{H} = \mathbb{C}^M \otimes \mathbb{C}^N = \mathbb{C}^{M \times N}$ . In the following we shall use the notation  $r(\rho)$  for the rank of the matrix  $\rho$  (which for a Hermitian matrix equals the number of its nonvanishing eigenvalues).

Performing the spectral decomposition of  $\rho$ ,

$$\rho = \sum_{l=1}^r \lambda_l |\psi_l\rangle\langle\psi_l|, \quad (1)$$

where  $\lambda_l$  are (positive) eigenvalues of  $\rho$ ,  $|\psi_l\rangle$  - its eigenvectors and  $r = r(\rho)$  - its rank. Defining  $|\Psi_l\rangle = \sqrt{\lambda_l} |\psi_l\rangle$  we thus decompose the nonnegative-definite Hermitian matrix  $\rho$  as a sum of rank-one operators,

$$\rho = \sum_{l=1}^r |\Psi_l\rangle\langle\Psi_l|. \quad (2)$$

The decomposition of (2) into the sum of rank-one operators is non-unique. Indeed the vectors

$$|\Phi_n\rangle = \sum_{l=1}^r W_{nl} |\Psi_l\rangle, \quad n = 1, \dots, K \geq r, \quad (3)$$

lead to another one,

$$\rho = \sum_{n=1}^K |\Phi_n\rangle\langle\Phi_n|, \quad (4)$$

involving  $K \geq r$  components, provided that the rectangular  $K \times r$  matrix  $W$  fulfills  $W^\dagger W = I$ , where  $I$  is the  $r \times r$  identity matrix, i.e.  $W$  belongs to the  $V_{K,r}$  manifold. In fact all possible decompositions (4) of  $\rho$  into the sum of rank-one operators can be obtained from the spectral decomposition of  $\rho$  (2) in such a way [18, 19].

**Gram decompositions.** Let  $\{|E_\nu\rangle\}_{\nu=1,\dots,M \times N}$  be a basis in  $\mathbb{C}^{M \times N}$ . Starting from the spectral decomposition (2) we obtain for the matrix elements of  $\rho$ :

$$\rho_{\mu\nu} = \langle E_\mu | \rho | E_\nu \rangle = \sum_{l=1}^r \langle E_\mu | \Psi_l \rangle \langle \Psi_l | E_\nu \rangle = \sum_{l=1}^r \bar{w}_\mu^l w_\nu^l = \langle w_\mu, w_\nu \rangle, \quad (5)$$

$$w_\nu := \begin{bmatrix} w_\nu^1 \\ w_\nu^2 \\ \vdots \\ w_\nu^r \end{bmatrix} \in \mathbb{C}^r, \quad w_\nu^l := \langle \Psi_l | E_\nu \rangle, \quad (6)$$

where  $\langle \cdot, \cdot \rangle$  is the standard Hermitian scalar product in  $\mathbb{C}^K$ . It means that a Hermitian positive definite matrix is the Gram matrix (i.e. the matrix of scalar products) of the vectors  $w_\nu$  defined above. A set of vectors  $\{w_\nu\}$  fulfilling (5) we will call a Gram system for  $\rho$ , and we will say that it provides a Gram decomposition of  $\rho$ . If we do not insist that the vectors  $w_\nu$  are elements of  $\mathbb{C}^r$  we can construct other Gram decompositions of  $\rho$ , so in this sense the Gram decomposition is non-unique. Indeed, defining

$$w'_\nu = V w_\nu, \quad (7)$$

where  $w'_\mu \in \mathbb{C}^K$ , with  $K \geq r$  and  $V \in \mathbb{M}_{K \times r}$  - a rectangular matrix fulfilling  $V^\dagger V = I$ , we have  $\rho_{\mu\nu} = \langle w'_\mu, w'_\nu \rangle$ . It is easy to prove that all Gram decompositions of the matrix  $\rho$  are obtained by the transformation (7) from the spectral one (2) and (6). In particular two Gram systems calculated from two decompositions (2) and (4) are connected by the relation (7) with  $V = \overline{W}$  (cf. (3)). In the following we will also use the fact that if two sets of vectors  $w'_\nu$  and  $w''_\nu$ ,  $\nu = 1, \dots, r$ ,  $w'_\nu \in \mathbb{C}^K$ ,  $w''_\nu \in \mathbb{C}^K$  are Gram systems for the same positive-definite matrix  $\rho$ , i.e.  $\langle w'_\mu, w'_\nu \rangle = \langle w''_\mu, w''_\nu \rangle$ , then there exists a unitary  $U$  acting in  $\mathbb{C}^K$  such that  $w''_\nu = U w'_\nu$  for  $\nu = 1, \dots, r$ .

**Gram decomposition in bipartite systems.** Let us now take advantage of the fact that  $\rho$  acts on a tensor product space, i.e. we chose the basis  $\{|E_\nu\rangle\}_{\nu=1,\dots,M \times N}$  in the form of product states  $|E_\nu\rangle = |e_m\rangle \otimes |f_n\rangle =: |e_m \otimes f_n\rangle$ ,  $m = 1, \dots, M$ ,  $n = 1, \dots, N$  and repeat the calculation of (5),

$$\rho_{ij,mn} = \langle e_i \otimes f_j | \rho | e_m \otimes f_n \rangle = \sum_{l=1}^r \langle e_i \otimes f_j | \Psi_l \rangle \langle \Psi_l | e_m \otimes f_n \rangle = \sum_{l=1}^r \bar{w}_{ij}^l w_{mn}^l = \langle w_{ij}, w_{mn} \rangle, \quad (8)$$

where now  $w_{mn}$ ,  $m = 1, \dots, M$ ,  $n = 1, \dots, N$  are vectors in  $\mathbb{C}^r$ , with components

$$w_{mn}^l = \langle \Psi_l | e_m \otimes f_n \rangle. \quad (9)$$

If we assume that  $\rho$  is of maximal rank  $r = MN$  (which for  $M \geq 3$  we take for granted in the following), then  $w_{mn}$  are linearly independent. In particular, for any fixed  $\tilde{m} \in \{1, \dots, M\}$  ( $\tilde{n} \in \{1, \dots, N\}$ ) the vectors  $w_{\tilde{m}n}$ ,  $n = 1, \dots, N$  ( $w_{m\tilde{n}}$ ,  $m = 1, \dots, M$ ) form a set of  $N$  ( $M$ ) linearly independent vectors in  $\mathbb{C}^K$ , respectively. In the special case  $M = 2$ , the first of the latter statements can be also assumed to hold, provided  $\rho$  is (non-trivially) supported in the  $2 \times N$  space. If this statement was not true, the density matrix  $\rho$  would have a product vector in its kernel. In such situation either  $\rho$  is entangled and not PPT, or if it is PPT, than it can be represented as a mixture of a separable part and a density matrix supported in  $2 \times (N - 1)$  dimensional space (for proofs and details see Ref. [24]).

**Relations between various Gram decompositions.** Let  $\{v_n\}_{n=1,\dots,N}$  form an arbitrary set of linearly independent vectors in  $\mathbb{C}^K$  (in particular, in the light of the above remark, we can choose  $v_n = w_{1n}$ ). We can always find a family of linear maps  $F_m : \mathbb{C}^K \rightarrow \mathbb{C}^K$ ,  $m = 1, \dots, M$ , such that

$$w_{mn} = F_m v_n, \quad (10)$$

Note that such  $F_m$ 's are uniquely defined only on the  $N$ -dimensional subspace of  $\mathbb{C}^K$  spanned by  $\{v_n\}_{n=1,\dots,N}$ . If we apply the same procedure to the decomposition (4) we will arrive at

$$w'_{mn} = F'_m v'_n, \quad (11)$$

with  $v'_n$ ,  $n = 1, \dots, N$  some linearly independent vectors in  $\mathbb{C}^K$  and appropriate  $F'_m$ .

The vectors  $w_{mn}$  and  $w'_{mn}$  are connected by (7), i.e.

$$F'_m v'_n = w'_{mn} = V w_{mn} = V F_m v_n. \quad (12)$$

Since both sets  $\{v_n\}$  and  $\{v'_n\}$ ,  $n = 1, \dots, N$  are linearly independent in, respectively,  $\mathbb{C}^r$  and  $\mathbb{C}^K$ , there exists a  $K \times r$  matrix  $\tilde{V}$  of maximal rank, such that  $v'_n = \tilde{V} v_n$  for  $n = 1, \dots, N$ . Consequently

$$V^\dagger F'_m \tilde{V} v_n = V^\dagger V F_m v_n = F_m v_n, \quad (13)$$

where we used  $V^\dagger V = I$ . We have thus shown the following

**Theorem 1** *For the two decompositions of the Gram vectors of the form (10) and (11) stemming from two decompositions of  $\rho$  into rank-one operators of the form (2) and (4) there exist two  $K \times r$  matrices  $\tilde{V}$  and  $V$ , the former of rank  $r$  and the latter fulfilling  $V^\dagger V = I$ , such that on the space spanned by (arbitrarily chosen)  $N$  linearly independent vectors  $v_n \in \mathbb{C}^r$  the equality*

$$V^\dagger F'_m \tilde{V} = F_m \quad (14)$$

holds. □

Obviously  $\tilde{V}$  depends on the choice of  $\{v_n\}$ .

### III. SEPARABILITY PROBLEM

**Gram decompositions for separable states.** Our goal is to characterize Gram decompositions for density matrices of bipartite separable quantum systems. Recall that separable defined on  $\mathcal{H}_A \otimes \mathcal{H}_B$  systems are characterized by the following

**Definition 1** *A state  $\rho$  is separable if and only if*

$$\rho = \sum_{i=1}^k p_i \rho_i^A \otimes \rho_i^B. \quad (15)$$

where  $\sum_i p_i = 1$ ,  $p_i \geq 0$ , whereas  $\rho_i^A$  and  $\rho_i^B$  are states on  $\mathcal{H}_A$  and  $\mathcal{H}_B$ , respectively.

The above expression means that  $\rho$  can be written as a convex combination of product states.

To achieve the goal observe that performing a decomposition of the type (2) for all matrices  $\rho_i^A$  and  $\rho_i^B$  in (15) and taking into account positivity of the coefficients  $p_i$  we obtain that a state  $\rho$  is separable if and only if it can be decomposed in the form of  $K$  rank-one operators proportional to projections on simple tensors.

$$\rho = \sum_{k=1}^K |\varphi_k\rangle\langle\varphi_k| \otimes |\psi_k\rangle\langle\psi_k| = \sum_{k=1}^K |\varphi_k \otimes \psi_k\rangle\langle\varphi_k \otimes \psi_k|, \quad (16)$$

where  $|\varphi_k\rangle \in \mathcal{H}_A$ ,  $|\psi_k\rangle \in \mathcal{H}_B$ .

Calculating matrix elements of  $\rho$  in local bases  $\{|e_i\rangle\}_{i=1,\dots,M}$  and  $\{|f_i\rangle\}_{i=1,\dots,N}$  in  $\mathcal{H}_A = \mathbb{C}^M$  and  $\mathcal{H}_B = \mathbb{C}^N$ , respectively, we obtain

$$\begin{aligned}\rho_{ij,mn} &= \langle e_i \otimes f_j | \rho | e_m \otimes f_n \rangle \\ &= \sum_{l=1}^K \langle e_i | \varphi_l \rangle \langle f_j | \psi_l \rangle \langle \varphi_l | e_m \rangle \langle \psi_l | f_n \rangle \\ &= \sum_{l=1}^K \bar{w}'_{ij} w'_{mn} = \langle w'_{ij}, w'_{mn} \rangle,\end{aligned}\tag{17}$$

where now

$$w'_{mn} = \begin{bmatrix} w'_{mn}{}^1 \\ w'_{mn}{}^2 \\ \vdots \\ w'_{mn}{}^K \end{bmatrix} = \begin{bmatrix} \varphi_1^m \psi_1^n \\ \varphi_2^m \psi_2^n \\ \vdots \\ \varphi_K^m \psi_K^n \end{bmatrix} = \begin{bmatrix} \varphi_1^m & & & \\ & \varphi_2^m & & \\ & & \ddots & \\ & & & \varphi_K^m \end{bmatrix} \begin{bmatrix} \psi_1^n \\ \psi_2^n \\ \vdots \\ \psi_K^n \end{bmatrix} = D_m v'_n,\tag{18}$$

$$\phi_l^m := \langle \varphi_l | e_m \rangle, \quad \psi_l^n := \langle \psi_l | f_n \rangle.\tag{19}$$

**Reformulation of the separability problem.** From (18) it is thus clear that for a separable state  $\rho$  on  $\mathbb{C}^M \otimes \mathbb{C}^N$  which can be decomposed into the sum of  $K$  rank-one product operators (16), there exist  $D_m \in \mathbb{M}_{K \times K}$ ,  $m = 1, \dots, M$ ,  $D_m$  - diagonal, and  $v'_n \in \mathbb{C}^K$ ,  $n = 1, \dots, N$ , such that

$$\rho_{ij,mn} = \langle D_i v'_j, D_m v'_n \rangle.\tag{20}$$

Eq.(20) is also a sufficient condition for separability, ie. if there exist  $v'_n \in \mathbb{C}^K$ ,  $n = 1, \dots, N$  and diagonal  $D_m \in \mathbb{M}_{K \times K}$ ,  $m = 1, \dots, M$  such that (20) is fulfilled, then  $\rho$  can be decomposed into rank-one separable states (16) with

$$|\varphi_l\rangle = \sum_{m=1}^M \overline{(D_m)_l} |e_m\rangle,\tag{21}$$

$$|\psi_l\rangle = \sum_{n=1}^N \overline{(v_n)_l} |f_n\rangle.\tag{22}$$

i.e.  $\rho$  is separable.

Indeed, define

$$\tilde{\rho} = \sum_{l=1}^K |\varphi_l \otimes \psi_l\rangle \langle \varphi_l \otimes \psi_l|,\tag{23}$$

with  $\varphi_l$  and  $\psi_l$  defined by (21) and (22). Then  $\tilde{\rho}$  is separable and an elementary calculation shows that  $\tilde{\rho}_{ij,mn} = \rho_{ij,mn}$ , and thus  $\rho = \tilde{\rho}$ .

Summarizing we can formulate thus the following theorem

**Theorem 2** *A state  $\rho$  is separable if and only if there exists a Gram decomposition of  $\rho$ ,*

$$\rho_{ij,mn} = \langle w_{ij}, w_{mn} \rangle,$$

$w_{ij} \in \mathbb{C}^K$  for some  $K$ , such that

$$w_{ij} = D_i v_j,$$

with  $N$  vectors  $\{v_1, \dots, v_N\} \in \mathbb{C}^K$  and  $M$  diagonal matrices  $D_1, \dots, D_M$  acting as operators on  $\mathbb{C}^K$ .  $\square$

Observe that we can assume that all diagonal matrices  $D_i$  are nonsingular. Indeed from (18) their diagonal elements are equal to the projections of the vectors  $|\phi_l\rangle$ , which constitute (a part of) the decomposition, onto the basis vectors  $|e_m\rangle$ . If any number of them vanish we can always adjust slightly the basis to make them taking non-zero values.

Invoking now Theorem 1 we obtain a

**Corrolary 1** A state  $\rho$  of the full rank  $r = MN$  is separable if and only if for some  $K \geq MN$ , there exist  $K \times r$  matrices  $\tilde{V}$  and  $V$  of which  $\tilde{V}$  is of maximal rank and  $V^\dagger V = I$ , and diagonal  $K \times K$  matrices  $D_1, \dots, D_M$ , such that

$$V^\dagger D_m \tilde{V} = F_m$$

holds on the space spanned by  $v_n$ ,  $n = 1, \dots, M$ , where  $w_{mn} = F_m v_n$  is a Gram system (9) for  $\rho$  calculated from its spectral decomposition (2).  $\square$

Before proceeding let us make a remark. Observe namely that in terms of the Gram decomposition (20) of a separable  $\rho$  the operation of partial transposition in  $\mathcal{H}_B$

$$\rho = \sum_{i=1}^k p_i \rho_i^A \otimes \rho_i^B \mapsto \rho^{T_B} = \sum_{i=1}^k p_i \rho_i^A \otimes (\rho_i^B)^T, \quad (24)$$

ie.  $\rho_{ij,mn} \mapsto \rho_{in,mj}$ , corresponds to the complex conjugation of the frame  $\{v_1, \dots, v_N\}$ , ie.

$$\{v_1, \dots, v_N\} \rightarrow \{\overline{v_1}, \dots, \overline{v_N}\}, \quad (25)$$

whereas a similar operation performed in  $\mathcal{H}_A$

$$\rho = \sum_{i=1}^k p_i \rho_i^A \otimes \rho_i^B \mapsto \rho^{T_A} = \sum_{i=1}^k p_i (\rho_i^A)^T \otimes \rho_i^B, \quad (26)$$

ie.  $\rho_{ij,mn} \mapsto \rho_{mj,in}$ , consists in

$$\{D_1, \dots, D_M\} \rightarrow \{\overline{D_1}, \dots, \overline{D_M}\}. \quad (27)$$

Indeed:

$$\begin{aligned} \rho_{ij,mn}^{T_B} &= \rho_{in,mj} = \langle D_i v_n, D_m v_j \rangle = \langle v_n, \overline{D_i} D_m v_j \rangle = \overline{\langle \overline{D_i} D_m v_j, v_n \rangle} = \langle D_i \overline{D_m} \overline{v_j}, \overline{v_n} \rangle \\ &= \langle \overline{D_m} D_i v_j, \overline{v_n} \rangle = \langle D_i \overline{v_j}, D_m \overline{v_n} \rangle, \\ \rho_{ij,mn}^{T_A} &= \rho_{mj,in} = \langle D_m v_j, D_i v_n \rangle = \langle v_j, \overline{D_m} D_i v_n \rangle = \langle v_j, D_i \overline{D_m} v_n \rangle = \langle \overline{D_i} v_j, \overline{D_m} v_n \rangle, \end{aligned}$$

where we used the fact that diagonal matrices commute and their Hermitian conjugation reduces to the complex one.

In Appendix A we discuss in detail the results of this section applied to an example of two qubit states, the so called Werner states.

#### IV. SEPARABILITY AND FULL FAMILIES OF COMMUTING NORMAL MATRICES

***K-separability and FFCNM.*** In forthcoming publications we will present applications of Corollary 1 to characterization of the bipartite entanglement for arbitrary systems. In the present paper we would like to concentrate on the separability of systems with  $M = 2$ , but before that we would like to use our results from the previous sections to formulate a novel SNC for separability. Let us assume that the investigated state  $\rho$  is  $K$ -separable, i.e. there exists a decomposition into exactly  $K$  rank-one product operators (16) and  $\rho$  can be cast in the form (20). Since we assumed that  $\rho$  is of maximal rank  $r = NM$  we have necessarily  $K \geq MN$ . From the previous consideration we now that the Gram vectors calculated with the help of this decomposition have the form  $w'_{mn} = D_m v'_n$ .

For an arbitrary decomposition of  $\rho$  into exactly  $K$  states given by (4) (where  $|\Phi_l\rangle$  need not to be product states), we obtain another Gram system  $w''_{mn} = \langle \Phi_l | e_m \otimes f_n \rangle \in \mathbb{C}^K$ .

The vectors  $w'_{mn}$  and  $w''_{mn}$  as forming two Gram systems for the same matrix  $\rho$  are connected via a unitary transformation

$$w''_{mn} = U w'_{mn} = U D_m v'_n. \quad (28)$$

Taking the above equality for two pairs of indices  $(m, n)$  and  $(k, n)$  we obtain:

$$M_{mk} w''_{kn} = w''_{mn}, \quad (29)$$

where

$$M_{mk} = U D_m (D_k)^{-1} U^\dagger. \quad (30)$$

Remember that without loosing generality we can assume nonsingularity of all matrices  $D_n$ . Consequently  $M_{km}$  are also nonsingular.

**SNC for separability and FFCNM.** The matrices  $M_{nm}$  are normal,  $[M_{km}, M_{km}^\dagger] = 0$ , and mutually commuting,  $[M_{km}, M_{lm'}] = 0$ . Both observations can be easily proved using the facts that all matrices  $D_m$  are diagonal and  $U$  is unitary. The above reasoning is summarized in the form of the following

**Theorem 3** *A necessary and sufficient condition for  $K$ -separability of  $\rho$  is the existence, for an arbitrary decomposition (4), of a full family of  $M(M-1)/2$  normal, commuting  $K \times K$  matrices  $M_{km}$  fulfilling (29) where  $w'_{mn}$  are appropriate Gram vectors for the decomposition (29).*

Necessity of the condition follows from the above remarks, and to prove the sufficiency let us assume that (29) is fulfilled for some family of normal, commuting matrices  $M_{km}$ . It is a standard fact from the linear algebra [23] that all matrices in such a family can be simultaneously diagonalized by a single unitary transformation,

$$U^\dagger M_{km} U = D_{km}. \quad (31)$$

According to the previous remarks we assume that  $M_{km}$  and, consequently,  $D_{km}$  are nonsingular. Now from (29) and (31)

$$D_{km} U^\dagger w''_{mn} = U^\dagger M_{km} U U^\dagger w''_{mn} = U^\dagger M_{km} w''_{mn} = U^\dagger w''_{kn}, \quad (32)$$

and defining  $v_n := U^\dagger w''_{1n}$ ,  $w_{kn} := U^\dagger w''_{kn}$ , we obtain

$$w_{kn} = (D_{1k})^{-1} v_n. \quad (33)$$

The vectors  $w_{kn}$  are Gram vectors for  $\rho$  as they are obtained by a single unitary transformation from the vectors  $w''_{kn}$  constituting some Gram decomposition of  $\rho$ . Equation (32) reveals their structure in the form sufficient for the separability of  $\rho$  according to Theorem 2.

## V. SEPARABILITY IN $2 \times N$ SYSTEMS AND NORMAL EXTENSIONS

The Theorem 3 simplifies significantly for  $2 \times N$  systems, because FFCNM consists of a single matrix, which has to fulfill

$$\hat{M} w''_{0n} = w''_{1n}. \quad (34)$$

In the following we will use 0, 1 instead of 1, 2 for numbering the components on the qubit side, which is more in accord with the custom to denote the basis states by  $|0\rangle$  and  $|1\rangle$ . From here we do not need to assume the nonsingularity of  $\rho$  - see the remarks preceding the formula (10).

In this section we study the consequences of (34). On one hand we use the present formulation to obtain particularly simple proofs of known separability criteria. On the other hand, we use known separability criteria to obtain non-trivial statements concerning existence of normal extensions of matrices, whose matrix elements are only partially known.

**Canonical forms and PPT condition.** Let us consider  $\rho$  in the canonical form [24] (see also Appendix B)

$$\rho = \begin{bmatrix} A & B \\ B^\dagger & I \end{bmatrix}. \quad (35)$$

where the positivity of  $\rho$  implies  $A = BB^\dagger + \Lambda\Lambda^\dagger$ , where  $\Lambda$  is some  $N \times p$  matrix, with  $p \geq r(\Lambda\Lambda^\dagger)$ . Obviously,  $p = 1$  necessarily, when  $r(\Lambda\Lambda^\dagger) = 1$ ; also one can always take the minimal  $p = r(\Lambda\Lambda^\dagger) = 1$ . We represent  $\Lambda\Lambda^\dagger = \sum_{n=1}^p |\Lambda_n\rangle\langle\Lambda_n|$ .

Similar considerations concern the partially transposed matrix, which reads

$$\rho^{TA} = \begin{bmatrix} A & B^\dagger \\ B & I \end{bmatrix}. \quad (36)$$

We consider here only the nontrivial case of states with the positive partial transpose (PPT states) - states which are not PPT are not separable. The positivity of  $\rho^{TA}$  requires now that  $A = B^\dagger B + \tilde{\Lambda}^\dagger \tilde{\Lambda}$ , where  $\tilde{\Lambda}$  is now a  $\tilde{p} \times N$  matrix, with  $\tilde{p} \geq r(\tilde{\Lambda}^\dagger \tilde{\Lambda})$ , and having analogous properties as  $p$  introduced above. We represent  $\tilde{\Lambda}^\dagger \tilde{\Lambda} = \sum_{n=1}^{\tilde{p}} |\tilde{\Lambda}_n\rangle\langle\tilde{\Lambda}_n|$ . The PPT condition can be thus stated as  $A - B^\dagger B \geq 0$ . More precisely, it must hold

$$A = BB^\dagger + \Lambda\Lambda^\dagger = B^\dagger B + \tilde{\Lambda}^\dagger \tilde{\Lambda}, \quad (37)$$

which implies that given  $\Lambda$ ,  $\tilde{\Lambda}$  are not independent, and related by the above constraint.

Let us now discuss several examples to show how the novel entanglement SNC works.

**Rank  $N$  matrices.** The results of Ref. [24] indicate that rank  $N$  PPT states are  $N$ -separable. The matrix  $\hat{M} = B$  then, and  $[B, B^\dagger] = 0$ .

**The case  $\rho = \rho^{TA}$ .** From Ref. [24] we gather also that when  $\rho = \rho^{TA}$ , then  $\rho$  is  $2N$ -separable. In this case  $B = B^\dagger$ ,  $\Lambda = \tilde{\Lambda}^\dagger$  and the matrix  $M$  can be written as

$$\hat{M} = \begin{bmatrix} B & \Lambda \\ \Lambda^\dagger & s \end{bmatrix}. \quad (38)$$

with  $N \times N$  matrix  $S$  to be determined. Obviously, taking  $s$  Hermitian provides the desired normal extension of  $\hat{M}$ .

**The case of  $2 \times 2$  and  $2 \times 3$  systems.** In the two qubit, or qubit-qutrit case, every separable matrix is  $K$ -separable, where  $K = \max(r(\rho), r(\rho^{TA}))$ . In particular for the full rank  $r(\rho) = 4$  ( $r(\rho) = 6$ ),  $K = 4$  [26] or  $K = 6$  (as shown in Appendix B), respectively. We have then

**Corrolary 2** For  $N = 2, 3$ , an arbitrary  $N \times N$  matrix  $B$ , and an arbitrary  $p \times N$  matrix  $\Lambda$  constrained by (37), the matrix

$$\hat{M} = \begin{bmatrix} B & \Lambda \\ \tilde{\Lambda} & s \end{bmatrix}. \quad (39)$$

is normal, i.e. there exist a  $p \times p$  matrix  $s$ , and a  $N \times p$  matrix  $\tilde{\Lambda}$  constrained by (37) such that  $\hat{M}$  is normal. This holds in particular for minimal  $p = \min 0, r(\rho) - N$ .

**Edge PPT entangled states for  $N = 4$ .** Perhaps the most interesting are applications for PPT entangled states, and in particular for the so called edge states [24], i.e. PPT states that cannot be represented as a mixture of a PPT state and a separable states (no separable part can be subtracted). Such states are extreme examples of states to which the range criterion of P. Horodecki [27] applies. For  $N = 4$  such states may have rank 5, or 6 (and similarly their partial transpose). From the analysis of the Appendix B we infer that if  $\rho$  is a separable state of rank 5 such that its partial transpose has rank 5 (6), then it is 5-separable (6-separable). In the case  $r(\rho) = r(\rho^{TA}) = 5$ , both  $\Lambda$  and  $\tilde{\Lambda}$  have rank 1; we denote  $\Lambda$  by  $|\Lambda\rangle$ , and  $\tilde{\Lambda}^\dagger$  by  $|\tilde{\Lambda}\rangle$ . We get then

**Corrolary 3** A PPT state  $\rho$  such that it and its partial transpose have rank 5 is separable, iff there exist a complex number  $s$  such that the matrix

$$\hat{M} = \begin{bmatrix} B & |\Lambda\rangle \\ \langle\tilde{\Lambda}| & s \end{bmatrix}. \quad (40)$$

is normal, which assuming that (37) holds, requires that

$$(B - s)|\tilde{\Lambda}\rangle = (B^\dagger - s^*)|\Lambda\rangle.$$

This condition is equivalent to the range criterion. For the particular example  $\rho_{97}$  of the  $2 \times 4$  state analyzed in the seminal 1997 paper [27], it is very easy to analyse, as we show in Appendix C.

This analysis may be extended to the rank 5 states, with the partial transpose of rank 6, for which Eq. (37) becomes

$$BB^\dagger + |\Lambda\rangle\langle\Lambda| = B^\dagger B + |\tilde{\Lambda}_1\rangle\langle\tilde{\Lambda}_1| + |\tilde{\Lambda}_2\rangle\langle\tilde{\Lambda}_2|. \quad (41)$$

We have in this case

**Corrolary 4** A PPT state  $\rho$  of rank 5, such that its partial transpose has rank 6, is separable, iff there exist complex numbers  $\alpha, \beta$ , such that  $|\alpha|^2 + |\beta|^2 = 1$ , and a  $2 \times 2$  matrix  $s$  such that the matrix

$$\hat{M} = \begin{bmatrix} B & \alpha|\Lambda\rangle & \beta|\Lambda\rangle \\ \langle\tilde{\Lambda}_1| & s_{11} & s_{12} \\ \langle\tilde{\Lambda}_2| & s_{21} & s_{22} \end{bmatrix}. \quad (42)$$

is normal, which assuming that (41) holds, requires that

$$(B - s_{11})|\tilde{\Lambda}_1\rangle - s_{21}|\tilde{\Lambda}_2\rangle = (\alpha B^\dagger - \alpha s_{11}^* - \beta s_{12}^*)|\tilde{\Lambda}\rangle,$$

$$(B - s_{22})|\tilde{\Lambda}_2\rangle - s_{12}|\tilde{\Lambda}_1\rangle = (\beta B^\dagger - \alpha s_{21}^* - \beta s_{22}^*)|\tilde{\Lambda}\rangle.$$



Before we end this section, we would like to stress that obviously the above discussion of normal extension of  $\hat{M}$  applies also to  $M \times N$  systems, if we focus on a single relation of the type (29), such as say

$$\hat{M}_{10}w''_{0n} = w''_{1n}. \quad (43)$$

The analysis pertains then to the study of separability on a particular  $2 \times N$  subspace of the full Hilbert space. In this sense it is somewhat similar to the theory of generalized concurrences of Ref. [22].

## VI. SUMMARY

We have presented a new approach to the separability problem by reformulating it in terms of existence of separable Gram decompositions of density matrices in auxiliary space. The existence of such Gram decompositions is equivalent to the existence of a full family of commuting normal matrices that relate components of Gram vectors. We have presented many examples and applications of this method mainly to the  $2 \times N$  systems. Several known separability criteria can be, on one hand, reproduced with this method in a particularly simple way, and on the other, can be used to derive nontrivial statements about the existence of FFCNM.

## Acknowledgments

We thank I. Cirac, F. Hulpke, Ph. Hyllus, J. Korbicz, B. Kraus, and A. Sanpera for helpful discussions. We acknowledge support of ESF PESC “QUDEDIS”, EU IP “SCALA”, Spanish MEC (FIS2005-04627 and Consolider Ingenio 2010 “QOIT”), and Polish grant PBZ-Min-008/P03/03.

## APPENDIX A: WERNER MATRICES FOR TWO QUBITS

As an example illustrating the results of Section III let us consider a one-parameter family of states for  $N = M = 2$

$$\rho = \frac{1}{4} \begin{bmatrix} 1+p & 0 & 0 & 2p \\ 0 & 1-p & 0 & 0 \\ 0 & 0 & 1-p & 0 \\ 2p & 0 & 0 & 1+p \end{bmatrix}, \quad (A1)$$

the so called Werner states [4]. The parameter  $p$  takes the values from the interval  $[0, 1]$ . One finds easily the spectral decomposition  $\rho = \sum_{i=1}^r |\Psi_i\rangle\langle\Psi_i|$  with

$$|\Psi_1\rangle = \begin{bmatrix} 0 \\ \sqrt{\frac{1-p}{8}} \\ -\sqrt{\frac{1-p}{8}} \\ 0 \end{bmatrix}, |\Psi_2\rangle = \begin{bmatrix} \sqrt{\frac{1-p}{8}} \\ 0 \\ 0 \\ -\sqrt{\frac{1-p}{8}} \end{bmatrix}, |\Psi_3\rangle = \begin{bmatrix} 0 \\ \sqrt{\frac{1-p}{8}} \\ \sqrt{\frac{1-p}{8}} \\ 0 \end{bmatrix}, |\Psi_4\rangle = \begin{bmatrix} \sqrt{\frac{1+3p}{8}} \\ 0 \\ 0 \\ \sqrt{\frac{1+3p}{8}} \end{bmatrix}, \quad (A2)$$

and calculates the Gram vectors (9)

$$w_{11} = \begin{bmatrix} 0 \\ \sqrt{\frac{1-p}{8}} \\ 0 \\ \sqrt{\frac{1+3p}{8}} \end{bmatrix}, w_{12} = \begin{bmatrix} \sqrt{\frac{1-p}{8}} \\ 0 \\ \sqrt{\frac{1-p}{8}} \\ 0 \end{bmatrix}, w_{21} = \begin{bmatrix} -\sqrt{\frac{1-p}{8}} \\ 0 \\ \sqrt{\frac{1-p}{8}} \\ 0 \end{bmatrix}, w_{22} = \begin{bmatrix} 0 \\ -\sqrt{\frac{1-p}{8}} \\ 0 \\ \sqrt{\frac{1+3p}{8}} \end{bmatrix}. \quad (A3)$$

We chose  $v_1 = w_{11}$  and  $v_2 = w_{22}$  which allows to take

$$F_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad F_2 = \begin{bmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{\frac{1-p}{1+3p}} \\ 0 & 0 & \sqrt{\frac{1+3p}{1-p}} & 0 \end{bmatrix}. \quad (A4)$$

Only when  $p \leq 1/3$  the state  $\rho$  is separable. For these values of  $p$  one finds an explicit Gram decomposition (20) of  $\rho$  with

$$D_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$D_2 = \begin{bmatrix} \frac{(1-i)(\sqrt{1-3p}+\sqrt{p+1})}{\sqrt{2}(\sqrt{1-p}+\sqrt{3p+1})} & 0 & 0 & 0 \\ 0 & -\frac{(1+i)(\sqrt{p+1}-\sqrt{1-3p})}{\sqrt{2}(\sqrt{1-p}-\sqrt{3p+1})} & 0 & 0 \\ 0 & 0 & -\frac{(1-i)(\sqrt{1-3p}+\sqrt{p+1})}{\sqrt{2}(\sqrt{1-p}+\sqrt{3p+1})} & 0 \\ 0 & 0 & 0 & \frac{(1+i)(\sqrt{p+1}-\sqrt{1-3p})}{\sqrt{2}(\sqrt{1-p}-\sqrt{3p+1})} \end{bmatrix},$$

and

$$v'_1 = \begin{bmatrix} \frac{(\sqrt{1-p}+\sqrt{3p+1})}{4\sqrt{2}} e^{\frac{\pi i}{2}} \\ \frac{(\sqrt{1-p}-\sqrt{3p+1})}{4\sqrt{2}} e^{\frac{\pi i}{2}} \\ \frac{(\sqrt{1-p}+\sqrt{3p+1})}{4\sqrt{2}} e^{-\frac{\pi i}{2}} \\ \frac{(\sqrt{1-p}-\sqrt{3p+1})}{4\sqrt{2}} e^{-\frac{\pi i}{2}} \end{bmatrix}, \quad v'_2 = \begin{bmatrix} \frac{(\sqrt{p+1}-\sqrt{1-3p})}{4\sqrt{2}} e^{\frac{3\pi i}{4}} \\ \frac{(\sqrt{1-3p}+\sqrt{p+1})}{4\sqrt{2}} e^{-\frac{3\pi i}{4}} \\ \frac{(\sqrt{p+1}-\sqrt{1-3p})}{4\sqrt{2}} e^{\frac{3\pi i}{4}} \\ \frac{(\sqrt{1-3p}+\sqrt{p+1})}{4\sqrt{2}} e^{-\frac{3\pi i}{4}} \end{bmatrix}.$$

For the particular choice of  $F_1, F_2, v_1$ , and  $v_2$  the matrices  $\tilde{V}$  and  $V$  (cf. Corollary 1) are given as

$$\tilde{V} = V = \begin{bmatrix} \frac{-\sqrt{1+p}+i\sqrt{1-3p}}{\sqrt{8}\sqrt{1-p}} & -\frac{i}{2} & \frac{\sqrt{1-3p}-i\sqrt{1+p}}{\sqrt{8}\sqrt{1-p}} & -\frac{i}{2} \\ \frac{-\sqrt{1+p}+i\sqrt{1-3p}}{\sqrt{8}\sqrt{1-p}} & -\frac{i}{2} & \frac{-\sqrt{1-3p}+i\sqrt{1+p}}{\sqrt{8}\sqrt{1-p}} & \frac{i}{2} \\ \frac{-\sqrt{1+p}+i\sqrt{1-3p}}{\sqrt{8}\sqrt{1-p}} & \frac{i}{2} & \frac{\sqrt{1-3p}-i\sqrt{1+p}}{\sqrt{8}\sqrt{1-p}} & \frac{i}{2} \\ \frac{-\sqrt{1+p}+i\sqrt{1-3p}}{\sqrt{8}\sqrt{1-p}} & \frac{i}{2} & \frac{-\sqrt{1-3p}+i\sqrt{1+p}}{\sqrt{8}\sqrt{1-p}} & -\frac{i}{2} \end{bmatrix}, \quad (\text{A5})$$

for which one easily checks  $V^\dagger D_m \tilde{V} = F_m$  on  $\text{span}(v_1, v_2)$ .

## APPENDIX B: A SHORT GUIDE TO $2 \times N$ SYSTEMS

From Theorem 3 it is clear that investigations of separability can be simplified if we know *a priori* the order of separability  $K$  of the given state (i.e. we know that it is  $K$ -separable). We do not have any general tool for determining exactly the order of separability for arbitrary separable states before finding their actual decomposition into pure products (and even if we find one, to establish the order of separability we still have to prove that the found decomposition involves the minimal number of components). Here we present some exact results concerning orders of separability in the case of  $2 \times N$  systems for low values of  $N$ .

**Canonical forms.** Let  $\rho$  be an arbitrary density matrix of a bipartite  $2 \times N$  system

$$\rho = \begin{bmatrix} A & B \\ B^\dagger & C \end{bmatrix}, \quad (\text{B1})$$

where  $A, B$  and  $C$  are  $N \times N$  matrices,  $A$  and  $C$  are hermitian due to hermiticity of  $\rho$ . Positive definiteness of  $\rho$  implies  $A \geq 0$ ,  $C \geq 0$ , and  $A - BC^{-1}B^\dagger \geq 0$ . The matrix  $C$  is nonsingular since  $\rho$ , by assumption, is of maximal rank. By an invertible transformation

$$\rho \mapsto (I \otimes C^{-1/2}) \rho (I \otimes C^{-1/2}) \quad (\text{B2})$$

we bring  $\rho$  to the *canonical form* [24]

$$\rho = \begin{bmatrix} A & B \\ B^\dagger & I \end{bmatrix}. \quad (\text{B3})$$

For simplicity of notation we kept the same symbols  $A$  and  $B$  to denote the appropriate blocks of  $\rho$  despite the fact that the original blocks defined in (B1) are altered by the transformation (B2). Such a transformation changes, in principle, the trace of  $\rho$ , but since the normalization of the trace does not influence separability properties we will wave this point aside. The positivity conditions of  $\rho$  reduce now to

$$A = BB^\dagger + \Lambda\Lambda^\dagger, \quad (\text{B4})$$

where  $\Lambda$  is some  $p \times N$  matrix.

A necessary criterion of separability is the non-negative definiteness of the partially transposed matrix, which for the case of a  $2 \times N$  system ( $2N$ ) is defined as

$$\rho^{T_A} = \begin{bmatrix} A & B^\dagger \\ B & I \end{bmatrix}. \quad (\text{B5})$$

From now on we will assume thus that both  $\rho$  and  $\rho^{T_A}$  are positive-definite (otherwise  $\rho$  is not separable). Positive definiteness of the partial transpose of (B3) demands

$$A = B^\dagger B + \tilde{\Lambda}^\dagger \tilde{\Lambda}, \quad (\text{B6})$$

for some  $\tilde{\Lambda}$ .

**Decompositions of  $\rho$ .** For our purposes it important to consider particular decompositions of  $\rho$  for  $K = N + p$ , and construct the "known" part of the matrix  $\hat{M}$  that fulfills Eq. (29). From the canonical form and Eq. (B4), with  $\Lambda = (|\Lambda_1\rangle, \dots, |\Lambda_p\rangle)$ , it is easy to see that  $\rho = \sum_{k=1}^{N+p} |\Phi_k\rangle\langle\Phi_k|$ , with

$$|\Phi_k\rangle = |0\rangle \otimes |k\rangle + |1\rangle \otimes B|k\rangle, \quad (\text{B7})$$

for  $k = 1, \dots, N$ , and

$$|\Phi_k\rangle = |1\rangle \otimes |\Lambda_{k-N}\rangle, \quad (\text{B8})$$

for  $k = N + 1, \dots, N + p$ . From this particular form we read the components of the vectors  $w''_{0n}, w''_{1n}$ :

$$(w''_{0n})^k = \delta_{kn}, \quad (\text{B9})$$

for  $k = 1, \dots, N$ , and zero otherwise. Similarly

$$(w''_{1n})^k = B_{nk}, \quad (\text{B10})$$

for  $k = 1, \dots, N$ , and

$$(w''_{1n})^k = \langle n | \Lambda_{k-N} \rangle, \quad (\text{B11})$$

for  $k = N + 1, \dots, N + p$ . Obviously, for the particularly simple form of  $w''_{0n}$ , Eq. (29), determines only the first  $N$  columns of the matrix  $\hat{M}^T$ , which are

$$\hat{M}^T = \begin{bmatrix} B^T & ? \\ \Lambda^\dagger & ? \end{bmatrix}, \quad (\text{B12})$$

where the other entries are at this moment not known. Transposing and using the PPT constraint (37), we indeed obtain that

$$\hat{M} = \begin{bmatrix} B & \Lambda \\ \tilde{\Lambda} & S \end{bmatrix}, \quad (\text{B13})$$

where for given  $B$  and  $\Lambda$ , the matrix  $\tilde{\Lambda}$  is constrained only by the condition (37), and  $S$  is completely arbitrary. This form of  $\hat{M}$  is intensively used by us in the section on separability in  $2 \times N$  systems.

**Edge states.** For the purpose of this paper we remind the reader the basic concept associated with the edge states. First, we remind [24, 25, 28] that if  $|e, f\rangle$  (or any vector, in fact) is in the range of  $\rho$ , then we can write

$$\rho = \rho' + \lambda |e, f\rangle\langle e, f|,$$

where  $\rho' \geq 0$  provided  $\lambda \leq 1/\langle e, f | \rho^{-1} | e, f \rangle$ . When the equality holds, the rank of  $\rho'$  is smaller than the rank of  $\rho$  by 1.

From this observation follows

**Corrolary 5** *A PPT state  $\rho$  is an edge state if there exist no product vector  $|e, f\rangle$  in its range, such that  $|e^*, f\rangle$  is in the range of  $\rho^{TA}$ .*

Subtracting projectors on product vectors as in Refs. [24, 28] allows to determine the minimal number of projectors on product states necessary to decompose a separable state. We remind the reader:

**The case  $2 \times 2$ .** In this case  $K = \max(r(\rho), r(\rho^{TA}))$ . This result stems from [26]. In the following we shall use notation  $(p, q)$  for the case of  $r(\rho) = p$ ,  $r(\rho^{TA}) = q$ . Let us consider the case of full ranks (4,4). First we show that we can find the product vector for which  $\lambda = 1/\langle e, f | \rho^{-1} | e, f \rangle = 1/\langle e^*, f | (\rho^{TA})^{-1} | e^*, f \rangle$ , so that subtracting projector on this vector reduces ranks to (3,3). To this aim we suppose  $\rho = \sum_{k=1}^K |e_k, f_k\rangle\langle e_k, f_k|$  is separable, and that for all  $|e, f\rangle$ , it holds  $\langle e, f | \rho^{-1} | e, f \rangle < \langle e^*, f | (\rho^{TA})^{-1} | e^*, f \rangle$ . Inserting into this inequality  $|e_k, f_k\rangle$  and summing over  $k$ , we get a contradiction  $Tr(I) = 4 < 4 = Tr(I)$ . In the same manner we prove that the opposite inequality can not be fulfilled by all product vectors. Thus either all product vectors fulfill the equality, or there are at least two product vectors for which the inequality takes opposite signs. But then from the Darboux property and the fact the set of all product states is connected, we gather that there exist a product vector for which the equality holds. In the next step we reduce one rank to 2; this, however implies that so does the other rank, since from general theory of Ref. [24] it follows that rank  $N$  PPT matrix in  $2 \times N$  systems is  $N$ -separable.

**The case  $2 \times 3$ .** This problem was partially addressed in the thesis of G. Vidal [29]. The proof here is new. We start with the full ranks and using the same argument as above we reduce the ranks to (5,5). The argument may be then repeated but with a certain care. Now we suppose that  $\rho = \sum_{k=1}^K |e_k, f_k\rangle\langle e_k, f_k|$  is separable, and that for all  $|e, f\rangle$  in its range, and such that  $|e^*, f\rangle$  is in the range of  $\rho^{TA}$ , it holds  $\langle e, f | \rho^{-1} | e, f \rangle < \langle e^*, f | (\rho^{TA})^{-1} | e^*, f \rangle$ . Again, inserting into this inequality  $|e_k, f_k\rangle$  and summing over  $k$ , we get a contradiction  $Tr(I_{R(\rho)}) = 5 < 5 = Tr(I_{R(\rho^{TA})})$ , where  $I_{R(\rho)}$  denotes identity on the range. We may again evoke the Darboux property, but to this aim we need to prove that the set of product vectors on question is connected. Let  $\Psi$  be a vector from the kernel of  $\rho$  and  $\Phi$  from the kernel of  $\rho^{TA}$ . The product vectors we look for have to fulfill  $\langle \Psi | e, f \rangle = 0$ ,  $\langle \Phi | e, f \rangle = 0$ . These equations can be regarded as two linear equations for a three-component vector  $|f\rangle$ , parametrized by the vector  $|e\rangle = |0\rangle + \alpha|1\rangle$ , which we have parametrized by complex number  $\alpha$  in some basis. Obviously,  $|f\rangle$  is a unique function of  $\alpha$  and by scanning  $\alpha$  over the complex plane we can reach any of these vectors in a continuous way. Darboux theorem says then that there exist a product vector for which equality holds  $\langle e, f | \rho^{-1} | e, f \rangle = \langle e^*, f | (\rho^{TA})^{-1} | e^*, f \rangle$ , and we can reduce the ranks to (4,4). The next step is as above: reduction of one of the ranks to 3, implies the same reduction for the other. The reason for that is that all rank 3 states in  $2 \times 3$  systems are 3-separable.

**The case  $2 \times 4$ .** It is also possible to determine what is the minimal number of terms in the separable decomposition for the states of low ranks. In this paper we consider two cases: (5,5) and (5,6). In the (5,5) case there are three vectors  $|\Psi_i\rangle$  in the kernel of  $\rho$ , and another three vectors  $|\Phi_i\rangle$  in the kernel of  $\rho^{TA}$ . We look for  $|e_k, f_k\rangle$  such that  $\langle \Psi_i | e, f \rangle = 0$ ,  $\langle \Phi_i | e^*, f \rangle = 0$  for all  $i = 1, 2, 3$ . These can be regarded as six linear equations for a four-component vector  $|f\rangle$ . They have solutions provided three  $4 \times 4$  determinants (constructed from the first three and one of the last three equations) vanish. These determinants constitute three polynomials of 3rd order in  $\alpha$  and first order in  $\alpha^*$ . Eliminating  $\alpha^*$  from them we obtain that two polynomials of 6th order in  $\alpha$  must vanish. Subtracting them with appropriate coefficients, we conclude that a polynomial of 5th order in  $\alpha$  must vanish, i.e. there are at most five product vectors having the desired properties. This implies that if  $\rho$  is separable, then it is 5-separable.

Similar analysis can be done for the case of the state  $\rho$  with the ranks (5,6). We end up then with one polynomial of 6th order in  $\alpha$ , i.e. we have at most six solutions, ergo if  $\rho$  is separable, then it is 6-separable. Note, that the states with ranks (5,6) are either separable, or entangled edge states, or mixtures of ranks (5,5) edge state with a single projector on a product vector from the range of  $\rho$ .

Unfortunately, only upper bounds on the number of product states in an decomposition of separable states are known for  $\rho$ 's of higher ranks. In particular, Caratheodory theorem (for proof see [27]) gives a general bound equal to the square of the dimension of the Hilbert space, i.e. in the present case  $(2 \times 4)^2 = 64$ , implying the every separable state is 64-separable.

For the states with ranks (5,7) it can be shown that there exists in the range of  $\rho$  a product vector  $(|0\rangle + \alpha|1\rangle)|f\rangle$ , such that  $(|0\rangle + \alpha^*|1\rangle)|f\rangle$  is in the range of  $\rho^{TA}$ . It is easy to see that the condition that these product vectors are orthogonal to the corresponding kernels of  $\rho$  and  $\rho^{TA}$ , leads to 4 linear equations for 4 components of  $|f\rangle$ . The

solutions of such equations exists if the determinant of the corresponding matrix vanishes. This matrix has three rows linear in  $\alpha$  and one row linear in  $\alpha^*$ , so that the determinant equations has the form

$$W_3(\alpha) + \alpha^* V_3(\alpha) = 0, \quad (\text{B14})$$

where  $W_3(\cdot)$  and  $V_3(\cdot)$  are polynomials of third order. Let us replace  $\alpha \rightarrow rs$ ,  $\alpha^* \rightarrow r/s$  with  $r > 0$  and  $s$  complex, and treat Eq. (B14) as an equation for  $s(r)$  (i.e. treating  $s$  as parametrically dependent on  $r$ ),

$$sW_3(rs) + rV_3(rs) = 0.$$

We will show that this equation has at least one root  $\alpha = rs$  with  $|s| = 1$ , i.e. with  $\alpha^* = r/s$ . To this aim we consider the asymptotic behavior at  $r \rightarrow \infty$ . It is easy to show that the above equation has three roots  $s_i = O(1/r) \rightarrow 0$ ,  $i = 1, 2, 3$  and one root  $s_4 = O(r) \rightarrow \infty$ . Analogously, for  $r \rightarrow 0$  it is easy to show that the equation has three roots  $\tilde{s}_i = O(1/r) \rightarrow \infty$ ,  $i = 1, 2, 3$  and one root  $\tilde{s}_4 = O(r) \rightarrow 0$ . All that implies that when we continuously change  $r$  from 0 to  $\infty$ , one the the three "large" roots must become "small". From continuity (i.e. again from the Darboux property) we get that for some  $r = r_0$ , the  $|s(r_0)| = 1$ . Unfortunately, we cannot say much more about the total number of such roots. Solving Eq. (B14) with respect to  $\alpha^*$ , complex conjugating the result, and stacking it back into Eq. (B14), we obtain an equation for  $\alpha^*$  of 10th order, which indicates that there are not more of than ten roots of Eq. (B14).

### APPENDIX C: HORODECKIS $2 \times 4$ EDGE STATE

In this Appendix we show how our method work for the famous state  $\rho_{97}$  introduced by P. Horodecki in the seminal paper [27]. In our notation this state has

$$B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \quad (\text{C1})$$

and

$$|\Lambda\rangle = \begin{bmatrix} \sqrt{(1-b)/2b} \\ 0 \\ 0 \\ \sqrt{(1+b)/2b} \end{bmatrix}, |\tilde{\Lambda}\rangle = \begin{bmatrix} \sqrt{(1+b)/2b} \\ 0 \\ 0 \\ \sqrt{(1-b)/2b} \end{bmatrix}. \quad (\text{C2})$$

This state has rank 5 (as its partial transpose) and is an example of an edge state [24]. As pointed in Ref. [27] there exist a unitary matrix  $K$ , such that  $K^2 = I$ ,  $KBK = B^\dagger$ , and  $K|\Lambda\rangle = |\tilde{\Lambda}\rangle$ . The condition of existence of the normal extension from Section VI reads then  $(B - s)|\tilde{\Lambda}\rangle = K(B - s^*)|\tilde{\Lambda}\rangle$ , i.e.

$$\begin{bmatrix} -s\sqrt{(1+b)/2b} \\ 0 \\ \sqrt{(1-b)/2b} \\ -s\sqrt{(1-b)/2b} \end{bmatrix} = \begin{bmatrix} -s^*\sqrt{(1-b)/2b} \\ \sqrt{(1-b)/2b} \\ 0 \\ -s^*\sqrt{(1+b)/2b} \end{bmatrix}, \quad (\text{C3})$$

which has only the two solutions  $s = 0$ ,  $b = 1$ , and the limiting case  $b = 0$ , with an arbitrary real  $s = s^*$ . These are exactly the two instances in which the Horodecki state is separable.

- 
- [1] see for instance D. Bruß and G. Leuchs (Eds.), *Lectures on Quantum Information*, (Wiley-VCH, Berlin, 2007).
  - [2] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, quant-ph/0702225, in print in Rev. Mod. Phys.
  - [3] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States*, (Cambridge University Press, Cambridge, 2006).
  - [4] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
  - [5] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Lett. **223**, 1 (1996).
  - [6] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
  - [7] K. Eckert, J. Schliemann, D. Bruss, and M. Lewenstein, Ann. Phys. (N.Y.) **299**, 88 (2002).
  - [8] Lu-Ming Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).

- [9] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
- [10] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac, Phys. Rev. Lett. **87**, 167904 (2001).
- [11] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac, Phys. Rev. A **64**, 052303 (2001).
- [12] For general description of the method see A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002); for a specific formulation of semi-definite approach for  $2 \times N$  systems see H.J. Woerdman, Phys. Rev. A **67**, 010303(R) (2003).
- [13] L. Gurvits, J. Comp. Sys. Sci. **69**, 448 (2004).
- [14] see for instance B. M. Terhal, Lin. Alg. Appl. **323**, 61 (2001); M. Lewenstein, B. Kraus, P. Horodecki, and J. I. Cirac, Phys. Rev. A **63**, 044304 (2001); H-P. Breuer, Phys. Rev. Lett. **97**, 080501 (2006).
- [15] see for instance B.M. Terhal, Theor. Comp. Sci. **287**, 313 (2002); M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000).
- [16] see for instance P. Horodecki and A. Ekert Phys. Rev. Lett. **89**, 127902 (2002); O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera Phys. Rev. A **66**, 062305 (2002); M. Bourennane, M. Eibl, Ch. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, Ph. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera Phys. Rev. Lett. **92**, 087902 (2004).
- [17] J. K. Korbicz and M. Lewenstein, Phys. Rev. A **74**, 022318 (2006).
- [18] E. Schrödinger, Naturwiss. **23**, 807 (1935).
- [19] L.P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. A **183**, 14 (1993).
- [20] M. Spivak, *A Comprehensive Introduction to Differential Geometry*, Vol. 5, (Publish or Perish, Wilmington, 1979).
- [21] J. Korbicz, PhD Thesis, Universität Hannover 2006.
- [22] F. Mintert, M. Kuś, and A. Buchleitner Phys. Rev. Lett. **92**, 167902 (2004).
- [23] R.A. Horn and Ch. R. Johnson, *Matrix Analysis*, (Cambridge University Press, Cambridge, 1990).
- [24] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein Phys. Rev. A **61**, 062302 (2000).
- [25] T. Wellens and M. Kuś, Phys. Rev. A **64**, 052302 (2001); S. Karnas and M. Lewenstein, J. Phys. A **34**, 6919 (2001).
- [26] A. Sanpera, R. Tarrach, and G. Vidal, Phys. Rev. A **58**, 826 (1998).
- [27] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
- [28] M. Lewenstein and A. Sanpera Phys. Rev. Lett. **80**, 2261 (1998).
- [29] G. Vidal, PhD Thesis, Universidad Barcelona 1999.